NOTICE: When government or other drawings, specifications or other data are used for any purpose other than in connection with a definitely related government procurement operation, the U. S. Government thereby incurs no responsibility, nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.

63-3-5

# A Few Probabilistic Properties of Modular Circuits

by
H. Kaneko

Series No. 60, Issue No. 448
Contract No. AF 19(604)-5466
April 30, 1962

ELECTRONICS RESEARCH LABORATORY
UNIVERSITY OF CALIFORNIA
BERKELEY, CALIFORNIA

AFCRL-62-939

Electronics Research Laboratory
University of California
Berkeley, California

# A FEW PROBABILISTIC PROPERTIES OF MODULAR CIRCUITS

by

H. Kaneko

Institute of Engineering Research
Series No. 60, Issue No. 448

Contract No. AF 19(604)-5466
Project No. 5632
Task No. 56320

Scientific Report No. 13

April 30, 1962

Prepared for
Electronics Research Directorate
Air Force Cambridge Research Laboratories
Office of Aerospace Research
United States Air Force
Bedford, Massachusetts

# ACKNOWLEDGMENT

I am greatly indebted to Prof. L. A. Zadeh, Prof. G. L. Turin and Prof. A. Gill for their instructive suggestions and encouragement on this work.

## ABSTRACT

Output probabilities of finite-state-machine elements are studied when the input of the machine elements is a random process. Delay element, modulo m adder and modulo m multiplier are considered as the machine elements. A new approach to the problem is made by defining the transformation matrices $\underline{T}$ and $\underline{U}_a$ for a modulo m adder and a modulo m multiplier respectively. By using these matrices, the output probabilities of the machine and the stochastic matrix of the output are given in explicit expressions, assuming that the input process is a finite-state, time-invariant Markov process. A few examples of the combinatorial circuit of these elements are also studied.

## TABLE OF CONTENTS

# I. INTRODUCTION

A few probabilistic input-output relations of finite-state-machine elements are derived for a random input. We defined the transformation matrices $\underline{T}$ and $\underline{U}_a$ in order to express the output probabilities in explicit relations, which are the matrices with entries of 1's and 0's. A few properties of these matrices are studied. $\underline{T}$ is the transformation matrix for the modulo m adder and $\underline{U}_a$ is that for the modulo m multiplier. If we restrict ourselves to a Galois field, or in other words, if m is a prime, we can obtain the consistent expressions for the probabilitistic relations both for the modulo m adder and for the modulo m multiplier.

Conditional probability of the two inputs of the machine is considered. In particular, modulo 2 multiplier is an input-dependent random switch. Combinatorial circuits using these modular circuit elements are analyzed in terms of the conditional probability and the absoute probability of the inputs. The stochastic matrix of the output of a few combinatorial circuits is also given in terms of the input stochastic matrix and the transition matrices we defined, when the input is a finite-state, time-invariant Markov process.

# II. BASIC ELEMENTS OF MODULAR CIRCUITS

We will consider a symbol x which belongs to a set of symbols S with m distinct component symbols such that

$$S = \{0, 1, 2, \dots, m-1\} \tag{2.1}$$

We define the absolute probability of a symbol x at time t as

$$\underline{P}_t(x) = \begin{bmatrix} P_t(x=0) \\ P_t(x=1) \\ \vdots \\ P_t(x=m-1) \end{bmatrix} \tag{2.2}$$

where

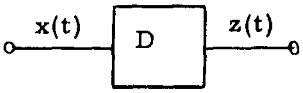
$$P_t(x) = \Pr(\mathrm{x} = x \text{ at time } t).$$

Suffix t will be omitted elsewhere through this paper unless it is necessary. Note that $\underline{P}_t(x)$ is not the function of x but rather of t as is seen in the definition (2. 2). However, we use this notation for convenience.

A. Delay Element

If we denote an input and an output at time t by x(t) and z(t), respectively, and the delay operator by D, then

$$z(t) = D\,x(t) = x(t-1) \qquad (2.\ 3)$$



Therefore, we have

$$\underline{P}_t(z) = \underline{P}_{t-1}(x) \qquad (2.\ 4)$$

where x, $z \epsilon$ S.

B. Modulo m Adder

We define an operator $\oplus$ of addition modulo m such that

$$z = a \oplus x \triangleq a + x \bmod m \qquad (2.\ 5)$$

where a, x, $z \epsilon$ S.

Example

| a\x | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

$z = a \oplus x \mod 5$

As is seen in the above example, the vector $\underline{z}$ is obtained by shifting the vector $\underline{x}$ by an amount equal to "a", cyclically to the descending direction of $\underline{x}$. Therefore, by defining a transformation $\underline{T}$ such that

$$\underline{T} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \quad m \times m \qquad (2.6)$$

we have the following relation:

$$\underline{P}(z \mid a) = \underline{T}^a \underline{P}(x), \qquad x, z, a \in S \qquad (2.7)$$

where $\underline{P}(z \mid a)$ is $\underline{P}(z)$ when "a" is known.

It is easy to see that $\underline{T}^a$ is a transformation which gives the one-to-one correspondence of x and z, because $\underline{T}^a$ has only one entry of 1 in each row and in each column and 0 elsewhere for any $a \in S$. Now, we have the basic relation

$$\underline{T}^a \underline{T}^b = \underline{T}^{a \oplus b} \qquad (2.8)$$

$\underline{T}$ is periodic with period m and

$$\underline{T}^m = \underline{T}^0 = \underline{I} = \text{identity matrix}$$

Also we can verify

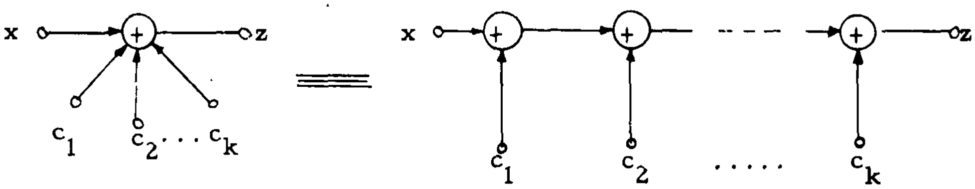
$$\sum_{k=0}^{m-1} \underline{T}^k = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \qquad (2.9)$$

$\underline{T}^a$ is an orthogonal matrix for all $a \in S$, because

$$\underline{T}^{a'} \underline{T}^a = \underline{I} \qquad \forall a \in S \qquad (2.10)$$

Therefore, $\underline{T}^a$ yields an orthogonal transformation of $\underline{P}(x)$.

More in general, if we consider a modulo m adder with one random input and k constant inputs $c_1, c_2, \ldots, c_k$ as depicted in the following figure, then the left side figure is equivalent to that of the right side, since the associative law holds for the operator $\oplus$.



Therefore, we have

$$\underline{P}(z \mid c_1, c_2, \ldots, c_k) = \underline{T}^{c_1} \underline{T}^{c_2} \ldots \underline{T}^{c_k} \underline{P}(x)$$
$$= \underline{T}^{c_1 \oplus c_2 \oplus \ldots \oplus c_k} \underline{P}(x) \qquad (2.11)$$

Next, we will consider a modulo m adder with two random inputs x and y. Then the output z is given by

$$z = x \oplus y$$

In general, x and y are not statistically independent and we define a conditional probability vector of x for a given y, such that

$$\underline{P}(x \mid y) = \begin{bmatrix} P(x=0 \mid y) \\ P(x=1 \mid y) \\ \vdots \\ P(x=m-1 \mid y) \end{bmatrix} \qquad (2.12)$$

Then, from eq. (2. 7), we have

$$\underline{P}(z \mid y) = \underline{T}^{y} \underline{P}(x \mid y)$$

Therefore, averaging this equation over all $y \epsilon S$, we get

$$\underline{P}(z) = \sum_{y=0}^{m-1} P(y) \underline{T}^{y} \underline{P}(x \mid y)$$

or equivalently

$$\underline{P}(z) = \sum_{x=0}^{m-1} P(x)\underline{T}^{x}\underline{P}(y \mid x) \tag{2.13}$$

In another expression, since a component of $\underline{P}(z)$ is the skew sum of the joint probability matrix of x and y, we can calculate it according to the following formula.

$$\begin{array}{l} P(z=0) \leftarrow \\ P(z=1) \leftarrow \\ \\ \\ P(z=m-1) \leftarrow \end{array} \begin{bmatrix} p(0,0) & p(0,1) & \cdots\cdots & p(0,m-1) \\ p(1,0) & p(1,1) & \cdots\cdots & p(1,m-1) \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots \\ p(m-1,0) & p(m-1,1) & \cdots\cdots & p(m-1,m-1) \end{bmatrix} \tag{2.14}$$

where p(x, y) is the joint probability of x and y.

Now, we define a transition matrix $\underline{G}$ such that

$$\underline{G} = [\,\underline{P}(x \mid 0),\ \underline{T}\ \underline{P}(x \mid 1),\ \underline{T}^{2}\ \underline{P}(x \mid 2), \ldots, \underline{T}^{m-1}\underline{P}(x \mid m-1)\,]$$

$$= \begin{bmatrix} P(0 \mid 0) & P(m-1 \mid 1) & \cdots & P(1 \mid m-1) \\ P(1 \mid 0) & P(0 \mid 1) & \cdots & P(2 \mid m-1) \\ P(2 \mid 0) & P(1 \mid 1) & \cdots & P(3 \mid m-1) \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots \\ P(m-1 \mid 0) & P(m-2 \mid 1) & \cdots & P(0 \mid m-1) \end{bmatrix}. \tag{2.15}$$

Then, using this matrix we can rewrite eq. (2.13) in an explicit formula;

$$\underline{P}(z) = \underline{G}\ \underline{P}(y) \tag{2.16}$$

$\underline{G}$' is an m by m matrix and is a stochastic matrix, which satisfies

$$\sum_{j=0}^{m-1} [\underline{G}']_{ij} = \sum_{i=0}^{m-1} [\underline{G}]_{ij} = 1 \tag{2.17}$$

This can easily be proved recalling that $\underline{T}^j$ is a transformation with one-to-one correspondence and that

$$\sum_{i=0}^{m-1} P(i|j) = 1$$

If x and y are statistically independent, then $P(x|y) = P(x)$ and

$$\underline{G} = [\underline{P}(x), \underline{T}\,\underline{P}(x), \underline{T}^2\,\underline{P}(x), \ldots, \underline{T}^{m-1}\,\underline{P}(x)]$$

$$= \begin{bmatrix} P(0) & P(m-1) & P(m-2) & \ldots\ldots & P(1) \\ P(1) & P(0) & P(m-1) & \ldots\ldots & P(2) \\ P(2) & P(1) & P(0) & \ldots\ldots & P(3) \\ \vdots & \vdots & \vdots & & \vdots \\ P(m-1) & P(m-2) & P(m-3) & \ldots\ldots & P(0) \end{bmatrix} \qquad (2.18)$$

From eq. (2.12) and knowing that $\underline{P}(x|y) = \underline{P}(x)$, we have

$$\underline{G} = \sum_{x=0}^{m-1} P(x)\,\underline{T}^x \qquad (2.19)$$

Also we see that

$$P(z) = \sum_{y} P(x = z-y \bmod m)\ P(y) \qquad (2.20)$$

This implies that P(z) is given by the composition modulo m of P(x) and P(y).

Furthermore, if

$$P(x|y) = P(x) = 1/m\ , \quad x \in S$$

then

$$G = \frac{1}{m}\sum_{x=0}^{m-1} T^x = \frac{1}{m} \cdot \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & 1 & 1 & \ldots & 1 \\ 1 & 1 & 1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \ldots & 1 \end{bmatrix} \qquad (2.21)$$

Therefore, $\underline{P}(z)$ is equal to $1/m$ for all $z \epsilon S$ regardless of $\underline{P}(y)$, i. e.,

$$\underline{P}(z) = \frac{1}{m}\begin{bmatrix}1\\1\\1\\ \vdots\\1\end{bmatrix} \tag{2.22}$$

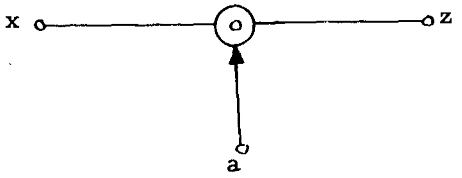
This is also true for any $\underline{P}(x)$ when $P(y) = 1/m$ for all $y \epsilon S$.

## C. Modulo m Multiplier

First, we will consider a constant multiplier defined by

$$z = a \circ x = ax \text{ mod } m \tag{2.23}$$

where a is a constant, x is a random input and z is an output of the multiplier as shown below.



As we have done for modulo m adder, we also define an m by m transformation matrix $\underline{U}_a$ such that

$$U_{a_{ij}} = \begin{cases}1, & i = a \circ j\\ 0, & i \neq a \circ j\end{cases} \tag{2.24}$$

$U_{a_{ij}}$ is ij-th element of the matrix $\underline{U}_a$. A few examples of $\underline{U}_a$ are shown in the appendix.

If $x = j$ is transformed by $\underline{U}_a$, then from eq. (2.24) z is given by $z = i = a \circ j$. Therefore, $\underline{U}_a$ is a transformation which gives the change of symbols from x to z according to $z = a \circ x$. The absolute probability vector of z for a given constant "a" is now given by

$$\underline{P}(z \mid a) = \underline{U}_a \underline{P}(x) \qquad (2.25)$$

Before going into the probabilistic relations of x, z and a, we will study more about $\underline{U}_a$.

i) $\underline{U}_a$ has exactly one entry of 1 in each column and 0 entries elsewhere.

Proof. Each of m input symbols has to make a deterministic transition to a certain output symbol in S. If there were two or more entries of 1's in a column, then there would be two or more outputs corresponding to that input. This contradicts the definition of deterministic machine elements. If there were no entry of 1 in a column, then there would be no output corresponding to the input. This contradicts the fact that the output symbol should be either one of the symbols in S. Therefore, there is exactly one entry of 1 in each column of $\underline{U}_a$ and 0 entries elsewhere. Q. E. D.

ii) Consequently, $\underline{U}_a$ has exactly m entries of 1's and $m^2$-m entries of 0's.

Now, we will prove the following theorem:

Theorem 1. If $a \neq 0$, then $\underline{U}_a$ has exactly one entry of 1 in each column and in each row, if and only if

$$\mathrm{GCD}(a, m) = 1, \quad a \in S, \quad a \neq 0 \qquad (2.26)$$

where GCD(a,m) denotes the Greatest Common Divisor of a and m.

Proof. From the definition of $\underline{U}_a$ by eq. (2.24),

$$i = a \circ j, \; j \in S, \quad a \in S, \; a \neq 0$$

then there exists a certain positive integer k such that

$$i = a \circ j = aj - km, \quad i \in S$$

Therefore, GCD(a, m) divides (aj-km) and hence, i; i.e.,

$$\frac{i}{GCD(a, m)} = a \circ j \quad \text{mod} \, \frac{m}{GCD(a, m)} \tag{2.27}$$

Now, m/GCD(a, m) is a prime. Recalling the theorem* of Galois field, i. e., for r, x, s $\epsilon$ S,

$$\left\{ \underset{s \neq 0}{\forall s} \, \forall r \;\; \exists\, x \, [x \circ s = r \bmod p] \right\} \Leftrightarrow \{p \text{ is prime}\} \tag{2.28}$$

we have

$$\left\{ \underset{a \neq 0}{\forall a} \, \forall \frac{i}{GCD(a, m)} \;\; \exists\, j \left[ \frac{i}{GCD(a, m)} = a \circ j \bmod \frac{m}{GCD(a, m)} \right] \right\}$$

$$\Leftrightarrow \left\{ \frac{m}{GCD(a, m)} \text{ is a prime, } a, \; j \epsilon S \right\} \tag{2.29}$$

The number of 1's in $\underline{U}_a$ is exactly m, and from the property (i) there is exactly one "1" associated with j for all j$\epsilon$ S. Therefore, i can take any integer in S, if and only if GCD(a, m) = 1. From the property (i), there is exactly one entry of 1 in j-th column for all j in S. Therefore, there is exactly one entry of 1 in the i-th row for all i$\epsilon$ S, if and only if GCD(a, m) = 1. Q. E. D.

Consequence. There is one-to-one correspondence between input symbols and output symbols, if and only if GCD(a, m) = 1.

Theorem 2. For all a, b$\epsilon$ S,

$$\underline{U}_a \underline{U}_b = \underline{U}_b \underline{U}_a = \underline{U}_{a \circ b} \tag{2.30}$$

Proof. Let us take a, b, i, j$\epsilon$ S, then by the definition of $\underline{U}_a$,

$$U_{a_{ik}} = \begin{cases} 1, & i = a \circ k \\ 0, & i \neq a \circ k \end{cases}$$

$$U_{b_{kj}} = \begin{cases} 1, & k = b \circ j \\ 0, & k \neq b \circ j \end{cases}$$

Since i is uniquely determined by i = a$\circ$b$\circ$j,

* See, Zadeh, L. A.,[1] Sept. 21, 1961. See also, Ref. 2.

$$[\underline{U}_a\underline{U}_b]_{ij} = \sum_{k=0}^{m-1} U_{a_{ik}} U_{b_{kj}} = U_{a_{ik}} U_{b_{kj}}$$

$$= \begin{cases} 1, & i = a \circ b \circ j \\ 0, & i \neq a \circ b \circ j \end{cases}$$

Therefore, by the definition of $\underline{U}_x$,

$$\underline{U}_a\underline{U}_b = \underline{U}_{a \circ b}$$

Furthermore, since $a \circ b = b \circ a$, we have

$$\underline{U}_{a \circ b} = \underline{U}_{b \circ a} = \underline{U}_b\underline{U}_a \qquad \text{Q. E. D.}$$

From these theorems, we can derive the following properties;

$$\underline{U}_m = \underline{U}_0 \tag{2. 31}$$

$$\underline{U}_0\underline{U}_k = \underline{U}_0, \text{ for all k; integer} \geq 0 \tag{2. 32}$$

$$\underline{U}_1 = \underline{I} \tag{2. 33}$$

$$\underline{U}_{m-k}^{n} = \underline{U}_{k}^{n}, \quad \forall k \in S, \quad n = \text{even integer} \tag{2. 34}$$

In particular,

$$\underline{U}_{m-1}^{2} = \underline{I}$$

<u>Theorem 3.</u> $\underline{U}_a$ is an orthogonal matrix, i. e.,

$$\underline{U}'_a\,\underline{U}_a = \underline{I} \tag{2. 35}$$

if and only if $a \neq 0$ and

$$\text{GCD}(a, m) = 1.$$

<u>Proof.</u>

$$[\underline{U}'_a\;\underline{U}_a]_{ij} = \sum_{k=0}^{m-1} U_{a_{ki}} U_{a_{kj}}$$

From the definition (2. 24) of $\underline{U}_a$,

$$U_{a_{ki}} U_{a_{kj}} = \begin{cases} 1, & k = a \circ i = a \circ j \\ 0, & \text{otherwise} \end{cases} \qquad a \neq 0$$

Recalling the theorem of Galois field* that

$$\{a \circ i = a \circ j \mod m\} \Longleftrightarrow \{i = j \mod \frac{m}{GCD(a, m)}\} \qquad (2. 36)$$

we have

$$[\underline{U}'_a \underline{U}_a]_{ij} = \begin{cases} 1, & i = j \mod \dfrac{m}{GCD(a, m)} \\ 0, & \text{otherwise} \end{cases}$$

Now, $i = j \mod m/GCD(a, m)$ is unique for $i, j \in S$, if and only if $GCD(a, m) = 1$. Therefore, $\underline{U}'_a \underline{U}_a = \underline{I}$, if and only if $a \neq 0$ and $GCD(a, m) = 1$. Q. E. D.

Consequently, we see that $\underline{U}_a$ is an orthogonal matrix for all $a \in S$ except $a = 0$, if m is a prime. Furthermore, $\underline{U}_1$ and $\underline{U}_{m-1}$ are orthogonal matrices for all integers $m \geq 2$.

In connection with the determinant of $\underline{U}_a$, we have the following theorem;

Theorem 4.

$$|\underline{U}_a| = \begin{cases} \pm 1, & \text{if } a \neq 0, \text{ and } GCD(a, m) = 1 \\ 0, & \text{if } a = 0, \text{ or } GCD(a, m) \neq 1. \end{cases}$$

Proof. For $a = 0$, it is evident that $|\underline{U}_0| = 0$. If $GCD(a, m) = 1$, from the theorem 1 there is exactly one entry of 1 in each column and in each row. Therefore, $\underline{U}_a$ is transformed to an identity matrix by a certain number of permutations of columns or rows. The value of the determinant does not change with such permutations except the sign of it, which is positive for an even number of permutations

* See, Zadeh, L. A.[1], Sept. 21, 1961. See also, Ref. 2.

and negative for an odd number of permutations. Since $|\underline{I}| = 1$, we have $|\underline{U}_a| = \underline{+}\,1$ if $a \neq 0$, and GCD(a, m) = 1.

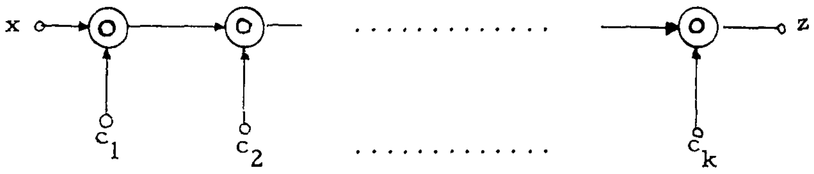
If GCD(a, m) $\neq$ 1, then by the theorem 1 there exist some rows whose entries are all zeroes. Therefore, the determinant of it is zero. Q. E. D.

Example.

$$\begin{array}{lllll}
m=3, & |\underline{U}_0|=0, & |\underline{U}_1|=1, & |\underline{U}_2|=-1 & \\
m=4, & |\underline{U}_0|=0, & |\underline{U}_1|=1, & |\underline{U}_2|=0, & |\underline{U}_3|=-1 \\
m=5, & |\underline{U}_0|=0, & |\underline{U}_1|=1, & |\underline{U}_2|=-1, & |\underline{U}_3|=-1 \\
 & |\underline{U}_4|=1 & & & \\
m=6, & |\underline{U}_0|=0, & |\underline{U}_1|=1, & |\underline{U}_2|=0, & |\underline{U}_3|=0 \\
 & |\underline{U}_4|=0, & |\underline{U}_5|=1 & &
\end{array}$$

Consequently, we can conclude that there exists an inverse matrix of $\underline{U}_a$, if and only if $a \neq 0$ and GCD(a, m) = 1.

So much for the general properties of $\underline{U}_a$, we will consider a cascaded connection of the constant multipliers with constants $c_1, c_2, c_3, \dots, c_k \in S$.



Then, from the theorem 2, we have the absolute probability of output z.

$$\begin{aligned}\underline{P}(z\,|\,c_1\ c_2\ \dots\ c_k) &= \underline{U}_{c_1}\underline{U}_{c_2}\cdots\underline{U}_{c_k}\underline{P}(x) \\ &= \underline{U}_{c_1\circ c_2\circ\cdots\circ c_k}\underline{P}(x)\end{aligned} \qquad (2.37)$$

Next, we will consider a modulo m multiplier with two random inputs x and y. By the similar fashion to that which we used for modulo m adder, we can get

$$\underline{P}(z \mid y) = \underline{U}_y \underline{P}(x \mid y) \tag{2. 38}$$

Therefore, we have

$$\underline{P}(z) = \sum_{y=0}^{m-1} P(y) \underline{U}_y \underline{P}(x \mid y)$$

or equivalently

$$\underline{P}(z) = \sum_{x=0}^{m-1} P(x) \underline{U}_x \underline{P}(y \mid x) \quad .$$

Defining a transition matrix $\underline{H}$ such that

$$\underline{H} = [\underline{U}_0 \underline{P}(x \mid 0), \underline{U}_1 \underline{P}(x \mid 1), \ldots, \underline{U}_{m-1} \underline{P}(x \mid m-1)] \tag{2. 40}$$

we can rewrite eq. (2. 36) in the form

$$\underline{P}(z) = \underline{H}\, \underline{P}(y) \tag{2. 41}$$

Here, $\underline{H}$ is an m by m square matrix and its transpose $\underline{H}'$ is a conditional probability matrix, which satisfies

$$\sum_{j=0}^{m-1} H'_{ij} = 1 \tag{2. 42}$$

This can be proved as follows:

From the definition of $\underline{H}$, we have

$$H_{ij} = \sum_{k=0}^{m-1} U_{j_{ik}} P(k \mid j)$$

Therefore,

$$\sum_{j=0}^{m-1} H'_{ij} = \sum_{i=0}^{m-1} H_{ij} = \left\{ \sum_{i=0}^{m-1} U_{j_{ik}} \right\} \left\{ \sum_{k=0}^{m-1} P(k|j) \right\}$$

From the property (i) of $\underline{U}_a$, we know that there is exactly one entry of 1 in each column of $\underline{U}_j$ for any $j \epsilon S$, hence, the column sum of $\underline{U}_j$ is equal to one. Also the second term of the above equation is one because $P(k|j)$ is a conditional probability. Therefore, we have

$$\sum_{j=0}^{m-1} H'_{ij} = 1 \qquad \text{Q. E. D.}$$

If x and y are statistically independent, then $P(x|y) = P(x)$ and

$$\underline{H} = [\underline{U}_0\underline{P}(x), \underline{U}_1\underline{P}(x), \ldots, \underline{U}_{m-1}\underline{P}(x)] \tag{2.43}$$

$$= \sum_{x=0}^{m-1} P(x)\underline{U}_x \tag{2.44}$$

Example: Independent case.

m=3

$$\underline{H} = \begin{bmatrix} 1 & P_0 & P_0 \\ 0 & P_1 & P_2 \\ 0 & P_2 & P_1 \end{bmatrix}$$

m=5

$$\underline{H} = \begin{bmatrix} 1 & P_0 & P_0 & P_0 & P_0 \\ 0 & P_1 & P_3 & P_2 & P_4 \\ 0 & P_2 & P_1 & P_4 & P_3 \\ 0 & P_3 & P_4 & P_1 & P_2 \\ 0 & P_4 & P_2 & P_3 & P_1 \end{bmatrix}$$

Further, if $P(x) = 1/m$ for all $x \epsilon S$, then from eq. (2.44)

$$\underline{H} = \begin{bmatrix} 1 & 1/m & 1/m & \ldots & 1/m \\ 0 & 1/m & 1/m & \ldots & 1/m \\ 0 & 1/m & 1/m & \ldots & 1/m \\ \vdots & \vdots & \vdots & & \\ 0 & 1/m & 1/m & \ldots & 1/m \end{bmatrix} \tag{2.45}$$

Therefore, we have

$$P(z) = \begin{cases} P(y=0) + \frac{1}{m}\sum_{i=1}^{m-1} P(y=i), & z = 0 \\ \\ \frac{1}{m}\sum_{i=1}^{m-1} P(y=i), & z \neq 0 \end{cases} \tag{2.46}$$

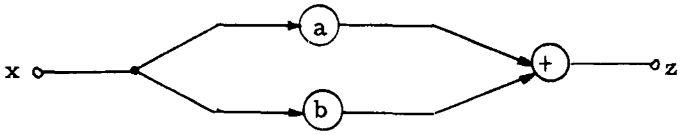
This shows us that if P(Y=0) is nonzero, the probability that z=0 is larger than the probability that z takes a symbol other than 0, which is equal for any symbols $z \in S$, $z \neq 0$.

Finally, we note that in particular for the binary system the modulo 2 multiplier is simply an on-off switch. If the two inputs are mutually correlated signals, the modulo 2 multiplier is a statistically input-dependent random switch.

## III. COMBINATORIAL CIRCUITS

We will study here a few examples of combinatorial circuits composed of the machine elements studied in the preceding articles.

### A. A Modulo m Adder and Two Constant Multipliers

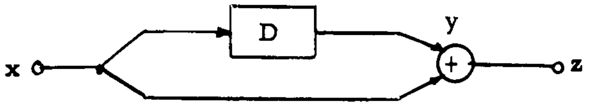


$$z = a \circ x \oplus b \circ x = (a \oplus b) \circ x \tag{3.1}$$

Therefore, this circuit is reduced to a circuit with a constant multiplier with constant $(a \oplus b)$. Hence, we have

$$\underline{P}(z \mid a, b) = \underline{U}_{a \oplus b}\underline{P}(x) \tag{3.2}$$

B. A Delay Element and a Modulo m Adder



$$y(t) = D\,x(t) = x(t-1)$$
$$z(t) = y(t) \oplus x(t) = x(t-1) \oplus x(t) \qquad (3.3)$$

The conditional probability P(x| y) is now

$$P\,[x(t) \mid y(t)\,] = P[x(t) \mid x(t-1)\,]$$

Therefore, if the input process is a time-invariant, finite-state simple Markov process, then $\underline{P}(x| y)$ is the column vector composed of the y-th column of the transpose of the stochastic matrix $\underline{p}$ of the input, i.e., defining

$$\underline{p}_y = \underline{P}(x| y) \qquad (3.4)$$

where the stochastic matrix $\underline{p}$ is

$$\underline{p}' = [\underline{p}_0, \underline{p}_1, \underline{p}_2, \ldots, \underline{p}_{m-1}] \qquad (3.5)$$

then, the absolute probability of z is

$$\underline{P}_t(z) = \underline{G}\ \underline{P}_t(y) = \underline{G}\ \underline{P}_{t-1}(x) \qquad (3.6)$$

where

$$\underline{G} = [\underline{p}_0,\ \underline{T}\,\underline{p}_1,\ \underline{T}^2\,\underline{p}_2, \ldots,\ \underline{T}^{m-1}\underline{p}_{m-1}] \qquad (3.7)$$

$\underline{G}$ is independent of time, since $\underline{p}$ is time-invariant. Using the property of a simple Markov process, i.e.,

$$\underline{P}_{t+1}\ (z) = \underline{G}\,\underline{P}_t(x) \qquad (3.8)$$

$$\underline{P}_t(x) = \underline{p}'\underline{P}_{t-1}(x) \qquad (3.9)$$

we have

$$\underline{P}_{t+1}(z) = \underline{G}\,\underline{p}'\,\underline{P}_{t-1}(x) \tag{3.10}$$

$$= \underline{G}\,\underline{p}'\,\underline{G}^{-1}\,\underline{P}_t(x)$$

$$= \{\underline{G}'^{-1}\underline{p}\,\underline{G}'\}'\;\underline{P}_t(z) \tag{3.11}$$

if $\underline{G}$ is nonsingular. This implies that if $|\underline{G}| \neq 0$ and x(t) is a simple Markov process, then the output z(t) is also a simple Markov process with stochastic matrix

$$\{\underline{G}'^{-1}\,\underline{p}\,\underline{G}'\} \tag{3.12}$$

<u>Example</u>: m=2

$$\underline{p} = \begin{bmatrix} 1-p_{01} & p_{01} \\ p_{10} & 1-p_{10} \end{bmatrix}$$

$$\underline{T} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\underline{G} = \begin{bmatrix} 1-p_{01} & 1-p_{10} \\ p_{01} & p_{10} \end{bmatrix}$$

$$|\underline{G}| = p_{10}-p_{01}$$

$$\underline{G}'^{-1} = \frac{1}{|\underline{G}|}\begin{bmatrix} p_{10} & -(1-p_{10}) \\ -p_{01} & (1-p_{01}) \end{bmatrix}$$

$$\underline{G}\underline{p}' = \begin{bmatrix} 1-p_{01}(1-p_{01}+p_{10}), & 1-p_{10}(1+p_{01}-p_{10}) \\ p_{01}(1-p_{01}+p_{10}), & p_{10}(1+p_{01}-p_{10}) \end{bmatrix} \tag{3.13}$$

$$\underline{G}'^{-1}\underline{p}\,\underline{G}' = \begin{bmatrix} 1-2p_{01}p_{10}, & 2p_{01}p_{10} \\ p_{01}+p_{10}-2p_{01}p_{10}, & 1-p_{01}-p_{10}+2p_{01}p_{10} \end{bmatrix} \tag{3.14}$$

We will see in this example that if the input process is an independent process, then

$$\underline{P}_{t+1}(z) = \underline{G}\,\underline{p}'\,\underline{P}_{t-1}(x) \tag{3.10}$$

$$= \underline{G}\,\underline{p}'\,\underline{G}^{-1}\,\underline{P}_t(x)$$

$$= \{\underline{G}'^{-1}\underline{p}\,\underline{G}'\}'\;\underline{P}_t(z) \tag{3.11}$$

if $\underline{G}$ is nonsingular. This implies that if $|\underline{G}| \neq 0$ and x(t) is a simple Markov process, then the output z(t) is also a simple Markov process with stochastic matrix

$$\{\underline{G}'^{-1}\,\underline{p}\,\underline{G}'\} \tag{3.12}$$

Example: m=2

$$\underline{p} = \begin{bmatrix} 1-p_{01} & p_{01} \\ p_{10} & 1-p_{10} \end{bmatrix}$$

$$\underline{T} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\underline{G} = \begin{bmatrix} 1-p_{01} & 1-p_{10} \\ p_{01} & p_{10} \end{bmatrix}.$$

$$|\underline{G}| = p_{10}-p_{01}$$

$$\underline{G}'^{-1} = \frac{1}{|\underline{G}|}\begin{bmatrix} p_{10} & -(1-p_{10}) \\ -p_{01} & (1-p_{01}) \end{bmatrix}$$

$$\underline{G}\underline{p}' = \begin{bmatrix} 1-p_{01}(1-p_{01}+p_{10}), & 1-p_{10}(1+p_{01}-p_{10}) \\ p_{01}(1-p_{01}+p_{10}), & p_{10}(1+p_{01}-p_{10}) \end{bmatrix} \tag{3.13}$$

$$\underline{G}'^{-1}\underline{p}\,\underline{G}' = \begin{bmatrix} 1-2p_{01}p_{10}, & 2p_{01}p_{10} \\ p_{01}+p_{10}-2p_{01}p_{10}, & 1-p_{01}-p_{10}+2p_{01}p_{10} \end{bmatrix} \tag{3.14}$$

We will see in this example that if the input process is an independent process, then

$p_{01}+p_{10}=1$

$$\underline{G'}^{-1}\underline{p}\,\underline{G'} = \begin{bmatrix} 1-2p_{01}p_{10}, & 2p_{01}p_{10} \\ 1-2p_{01}p_{10}, & 2p_{01}p_{10} \end{bmatrix} \qquad (3.15)$$

and, hence, z(t) is also an independent process. If $|\underline{G}|=0$, then $p_{01}=p_{10}$ and $\underline{G}^{-1}$ does not exist, and $P(x=0)=P(x=1)=1/2$.

$$\underline{G}\,\underline{p}'=\begin{bmatrix} 1-p_{01} & 1-p_{01} \\ p_{01} & p_{01} \end{bmatrix} \qquad (3.16)$$

and we have

$$\underline{P}_{t+1}(z) = \begin{bmatrix} 1-p_{01} \\ p_{01} \end{bmatrix} = \begin{bmatrix} p_{10} \\ 1-p_{10} \end{bmatrix} \qquad (3.17)$$

regardless of $\underline{P}(x)$ and t.

In general, if x(t) is an independent process, z(t) is also an independent process, when $|\underline{G}| \neq 0$. The proof of this statement is given as follows:

If x(t) is an independent process, then $p_{ij}=p_j$ and

$$\underline{G}'= \begin{bmatrix} p_0 & p_1 & p_2 & \cdots\cdots & p_{m-1} \\ p_{m-1} & p_0 & p_1 & \cdots\cdots & p_{m-2} \\ p_{m-2} & p_{m-1} & p_0 & \cdots\cdots & p_{m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_1 & p_2 & p_3 & \cdots\cdots & p_0 \end{bmatrix} \qquad (3.18)$$

Therefore, $\{\underline{p}\,\underline{G}'\}_{ij}=\{\underline{p}\,\underline{G}'\}_j$ is independent of i.

$$\{\underline{G}'^{-1}\underline{p}\,\underline{G}'\}_{ij} = \sum_{k=0}^{m-1} \{\underline{G}'^{-1}\}_{ik}\{\underline{p}\,\underline{G}'\}_{kj}$$

$$= \{\underline{p}\,\underline{G}'\}_j \sum_{k=0}^{m-1} \{\underline{G}'^{-1}\}_{ik}$$

Now, the second term of the above equation is

$$\sum_{j=1}^{m-1} [\underline{G}'^{-1}]_{ij} = \frac{1}{|\underline{G}|} \cdot \sum_{j=0}^{m-1} (-1)^{1+j} \, |\text{Cofac } G'_{ji}|$$

$$= \frac{1}{|\underline{G}|} \left| \underline{G}' \right|_{\text{i-th column replaced by 1's.}}$$

$$\triangleq |\underline{G}'_i| \, / \, |\underline{G}|$$

From eq. (3.18), we know that

$$\{\underline{G}'\}_{ij} = p_k, \quad k = j - i \mod m$$

Therefore,

$$\{\underline{G}'_n\}_{ij} = \begin{cases} 1, & i = n \\ p_k, & k = j - i \mod m, \quad i, j \in S, \quad i \neq n \end{cases}$$

Since $|\underline{G}'_n|$ does not change by an even number of permutations of $\underline{G}'_n$, by shifting the rows and columns of it by n, i.e., defining

$$r = i - n \mod m, \qquad s = j - n \mod m$$

we have

$$\{\underline{G}'_n\}_{ij} = \{\underline{G}'_0\}_{rs} = \begin{cases} 1, & r = 0 \\ p_k, & k = j - i = s - r \mod m \\ & i \neq n, \quad r \neq 0 \end{cases}$$

Hence, we have

$$\sum_{j=0}^{m-1} \{\underline{G}'^{-1}\}_{ij} = |\underline{G}'_n| \, / \, |\underline{G}| = |\underline{G}'_0| \, / \, |\underline{G}| = \text{Constant.} \quad \forall i \in S$$

Therefore,

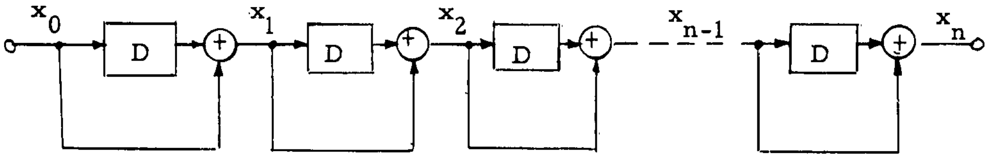
$$\{\underline{G}'^{-1}\underline{p}\,\underline{G}'\}_{ij} = \{\underline{G}'^{-1}\underline{p}\,\underline{G}'\}_{j}$$

Thus, completing the proof. Q. E. D.

If $|\underline{G}| = 0$, then $\underline{G}^{-1}$ does not exist and $\underline{P}_t(z)$ should be found from eq. (3. 6).

C. Cascaded Circuit of (B)

The analysis of the preceding example can be applied for the cascaded circuit shown below.



By the similar fashion we have

$$\underline{P}_t(x_n) = \underline{p}^{(k)'}\,\underline{P}_{t-1}(x_n) \tag{3.19}$$

where

$\underline{p}^{(0)} = \underline{p}$; stochastic matrix of the input process

$$\underline{p}^{(n)} = \underline{G}^{(n-1)'^{-1}}\,\underline{p}^{(n-1)}\,\underline{G}^{(n-1)'} \tag{3. 20}$$

$$= \underline{G}^{(n-1)'^{-1}}\,\underline{G}^{(n-2)'^{-1}} \cdots\cdots \underline{G}^{(0)'^{-1}}\,\underline{p}\,\underline{G}^{(0)'} \cdots\cdots \underline{G}^{(n-1)'}$$

$$\underline{G}^{(k)} = [\underline{p}_0^{(k)},\ \underline{T}\,\underline{p}_0^{(k)}, \ldots\ldots,\ \underline{T}^{m-1}\,\underline{p}_{m-1}^{(k)}\ ] \tag{3. 21}$$

$$\underline{G}^{(0)} = \underline{G}$$

By an iterative method one can find the stochastic matrix at the n-th stage. Furthermore, from eq. (3. 6), we have

$$\underline{P}_t(x_n) = \underline{G}^n\underline{P}_{t-n}(x_0)$$

If we consider a cascaded circuit with infinite number of unit circuits, then

$$\lim_{n\to\infty} \underline{P}_t(x_n) \triangleq P_\infty(x_\infty) = \underline{G}^\infty \underline{P}_0\,(x_0) \tag{3.23}$$

where

$$\underline{G}^\infty \triangleq \lim_{n\to\infty} \underline{G}^n \tag{3.24}$$

Since $\underline{G}'$ is a stochastic matrix and so is $\underline{G}'^n$, $\underline{G}^\infty$ can be found by the same way as we use to find the stationary solution of the absolute probability $\underline{Q}$ of a Markov process, whose transition matrix is $\underline{G}'$. Therefore, we have(6,.8, 9, 11)

$$\underline{G}^\infty = [\underbrace{\underline{Q}\;\underline{Q}\;\underline{Q}\ldots\ldots\underline{Q}}_{m}] \tag{3.25}$$

where $\underline{Q}$ is an eigenvector corresponding to the eigenvalue $\lambda=1$ of the characteristic equation

$$|\lambda\underline{I}-\underline{G}'| = 0 \tag{3.26}$$

and $\underline{Q}$ is uniquely determined from the condition that

$$\sum_{i=0}^{m-1} Q_i = 1.$$

<u>Example:</u> $m = 2$

$$\underline{G}' = \begin{bmatrix} 1-p_{01} & p_{01} \\ 1-p_{10} & p_{10} \end{bmatrix}$$

$$\underline{Q} = \frac{1}{1-p_{10}p_{01}} \begin{bmatrix} 1-p_{10} \\ p_{01} \end{bmatrix}$$

$$\underline{G}'^{\infty} = \frac{1}{1-p_{10}\,p_{01}} \begin{bmatrix} 1-p_{10} & p_{01} \\ 1-p_{10} & p_{01} \end{bmatrix}$$

This result indicates that the output absolute probability of infinitely cascaded networks of this type is independent of the probability of the input process and

$$\underline{P}_{\infty}(z) = \underline{Q}$$

Note that the delay introduced through this circuit is infinity.

State equation of the cascaded network with length n is written by

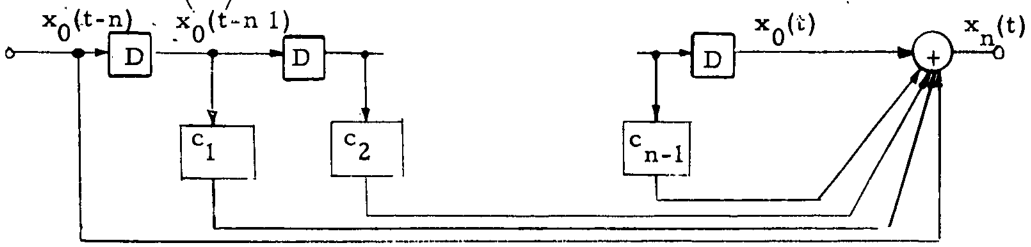
$$x_n(t) = x_{n-1}(t) \oplus x_{n-1}\ (t-1)$$

and we can also express it in terms of $x_0(t-i)$, i. e.,

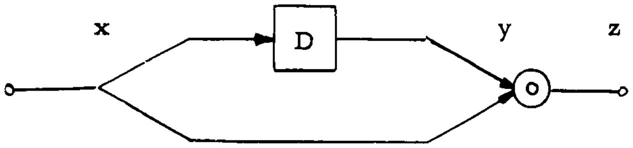
$$x_n(t) = \sum_{\substack{\oplus \\ j=0}}^{n} \binom{n}{i} \circ x_0(t-i) \qquad (3.27)$$

Accordingly, we can describe an equivalent circuit with n delay elements and (n-1) constant multipliers with constants $c_i$'s.

$$c_i = \binom{n}{i} \text{mod } m$$



### D. Delay Element and Modulo m Multiplier



$$z(t) = y(t) \circ x(t) = x(t-1) \circ x(t) \tag{3.28}$$

Assuming that x(t) is a time-invariant, simple Markov process, and using the matrices defined in the preceding article, we have

$$\underline{P}_t(z) = \underline{H}\,\underline{P}_{t-1}(x) \tag{3.29}$$

where $\underline{H}$ is, for this particular case,

$$\underline{H} = [\underline{U}_0\underline{p}_0, \underline{U}_1\underline{p}_1, \underline{U}_2\underline{p}_2, \ldots, \underline{U}_{m-1}\underline{p}_{m-1}] \tag{3.30}$$

$\underline{p}_k$ is defined by eq. (3.4) from the stochastic matrix of the input process. Similar to the preceding example, we have

$$\underline{P}_{t+1}(z) = \underline{H}\,\underline{p}'\,\underline{P}_{t-1}(x) \tag{3.31}$$

$$\underline{P}_{t+1}(z) = \{\underline{H}'^{-1}\,\underline{p}\,\underline{H}'\}'\underline{P}_t(z) \tag{3.32}$$

This implies that if the input process is a simple Markov process and $|\underline{H}| \neq 0$, then the output process is also a simple Markov process with stochastic matrix

$$\{\underline{H}'^{-1}\,\underline{p}\,\underline{H}'\} . \tag{3.33}$$

<u>Example:</u> m=2

$$\underline{p} = \begin{bmatrix} 1 - p_{01} & p_{01} \\ p_{10} & 1-p_{10} \end{bmatrix}$$

$$\underline{U}_0 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\underline{U}_1 = \underline{I}$$

$$\underline{H} = \begin{bmatrix} 1 & p_{10} \\ 0 & 1 - p_{10} \end{bmatrix}$$

$$|\underline{H}| = 1 - p_{10}$$

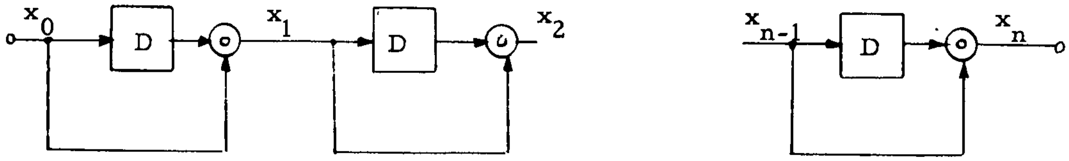
$$\underline{H}^{-1} = \frac{1}{1-p_{10}} \begin{bmatrix} 1-p_{10} & -p_{10} \\ 0 & 1 \end{bmatrix}$$

$$\underline{H}\,\underline{p}' = \begin{bmatrix} 1-p_{01}(1-p_{10}) & 2p_{10}-p_{10}^2 \\ p_{01}(1-p_{10}) & (1-p_{10})^2 \end{bmatrix} \tag{3.34}$$

$$\underline{H}'^{-1}\,\underline{p}\,\underline{H}' = \begin{bmatrix} 1-p_{01}(1-p_{10}) & p_{10}(1-p_{10}) \\ p_{10}(1+p_{01}) & 1-p_{10}(1+p_{01}) \end{bmatrix} \tag{3.35}$$

From this we can see that if the input process is an independent process, then $p_{01}+p_{10} = 1$ and the output process is also an independent process.

E. Cascaded Circuit of (D)



If we define the state vectors as in the above figure, then

$$x_n(t) = x_{n-1}(t) \circ x_{n-1}(t-1)$$

$$x_{n-1}(t) = x_{n-2}(t) \circ x_{n-2}(t-1)$$

........................

and finally we have

$$x_n(t) = \prod_{k \overset{\circ}{=} 0}^{n} \{x_0(t-k)\}^{c_k \circ} \tag{3.56}$$

where

$$x^{c\circ} = \underbrace{x \circ x \circ x \circ \cdots\cdots \circ x}_{c}$$

$$\prod_{k \overset{\circ}{=} 0}^{n} x_k = x_0 \circ x_1 \circ x_2 \circ \cdots\cdots \circ x_n$$

$$c_k = \binom{n}{k}$$

The results are quite similar to the example in (C).

$$\underline{P}_t(x_n) = \underline{p}^{(n)'} \underline{P}_{t-1}(x_n) \tag{3.57}$$

where

$$\underline{p}^{(0)} = \underline{p}$$

$$\underline{p}^{(n)} = \underline{H}^{(n-1)'^{-1}} \underline{p}^{(n-1)} \underline{H}^{(n-1)'}$$

$$= \underline{H}^{(n-1)'^{-1}} \underline{H}^{(n-2)'^{-1}} \cdots \underline{H}^{(0)'^{-1}} \underline{p} \underline{H}^{(0)'} \cdots \underline{H}^{(n-1)'}$$

$$\underline{H}^{(k)} = [\underline{U}_0 \underline{p}_0^{(k)}, \underline{U}_1 \underline{p}_1^{(k)}, \ldots\ldots, \underline{U}_{m-1} \underline{p}_{m-1}^{(k)}]$$

$$\underline{H}^{(0)} = \underline{H}$$

Then the input-output relation is given by

$$\underline{P}_t(x_n) = \underline{H}^n \underline{P}_{t-n}(x_0) \tag{3.58}$$

Also the limiting absolute probability $\underline{P}_\infty(x_\infty)$ is

$$\underline{P}_\infty(x_\infty) = \underline{Q}$$

where

$$\underline{H}^\infty = [\underbrace{\underline{Q}\ \underline{Q}\ \underline{Q} \cdots\cdots \underline{Q}}_{m}] \tag{3.59}$$

and $\underline{Q}$ is the stationary solution of the Markov process, which satisfies

$$(\underline{I}-\underline{H})\,\underline{Q}=\underline{0} \tag{3.60}$$

<u>**Example:**</u> m=2

$$\underline{H}=\begin{bmatrix}1 & p_{10}\\ 0 & 1-p_{10}\end{bmatrix}$$

$$\underline{Q}=\begin{bmatrix}1\\ 0\end{bmatrix}=\underline{P}_{\infty}(x_{\infty})$$

$$\underline{H}^{\infty}=\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}$$

In general we have

$$\underline{H}^{\infty}=\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 0 & 0 & 0 & \cdots & 0\\ 0 & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & & \vdots\\ 0 & 0 & 0 & \cdots & 0\end{bmatrix}=\underline{U}_0 \tag{3.61}$$

$$\underline{P}_{\infty}(x_{\infty})=\begin{bmatrix}1\\ 0\\ 0\\ \vdots\\ 0\end{bmatrix} \tag{3.62}$$

This implies that the output symbol is 0 with probability 1 as n approaches infinity. It is quite natural because "0" is an absorbing state through this network, and by an infinitely large number of trials through these network elements, the symbol at the final stage is absorbed in "0."

## IV. CONCLUSIONS

We have studied the transformation matrices $\underline{T}$ and $\underline{U}_a$ and their properties. Further, defining the transition matrices $\underline{G}$ and $\underline{H}$ for a modulo m adder and for a modulo m multiplier derived from $\underline{T}$ and $\underline{U}_a$, the output probabilities are expressed simply by the product of these matrices and the input probability matrix.

Also we have studied a few examples of the combinatorial circuit using these modular circuit elements. Circuits with delay elements are particularly of our interest. We have shown, in a few examples, that if the input process is a time-invariant simple Markov process, then the output process is also a simple Markov process whose stochastic matrix is iteratively found from the input stochastic matrix.

Combinatorial circuits with feedback are not treated yet in this paper. The same approach would be applied for a circuit with feedback, which is now being studied. If we obtain some expressions for them, it would be possible to generalize this analysis for a general modular system.

In a digital communication system, or in a digital data processing system, one may assume a digital computer or a sequential circuit at the terminal machines of it. Its input will be a stochastic process. Then, what would be an output process? This question is not wholly answered yet, because the circuit with feedback is not analyzed yet. It would be very interesting to analyze the probabilistic properties of such systems in order to design a desired circuit or to optimize a system in a probabilistic sense.

# APPENDIX

**Examples of $\underline{U}_a$:**

m = 2

$$\underline{U}_0 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\underline{U}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

m = 3

$$\underline{U}_0 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\underline{U}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\underline{U}_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

m = 4

$$\underline{U}_0 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\underline{U}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\underline{U}_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\underline{U}_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

m = 5

$$\underline{U}_0 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\underline{U}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\underline{U}_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$\underline{U}_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\underline{U}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

m = 6

$$\underline{U}_0 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\underline{U}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\underline{U}_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\underline{U}_3 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\underline{U}_4 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\underline{U}_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

## REFERENCES

1. Zadeh, L. A. et al., EE290 lectures, Fall 1961, at the University of California, Berkeley.
2. Peterson, W. W., Error Correcting Code, M. I. T. Press and John Wiley and Sons, 1961.
3. Shannon, C. E. and McCarthy, J. M., Automata Studies, Princeton University Press, 1956.
4. Kemeny, J. G. and Snell, J. L., Finite Markov Chains, D. Van Nostrand Co., 1960.
5. Fano, R. M., Transmission of Information, M. I. T. Press and John Wiley and Sons, 1961.
6. Bellman, R., Introduction to Matrix Analysis, McGraw-Hill, 1960.
7. Feller, W., An Introduction to Probability Theory and its Applications, Vol. I, John Wiley and Sons, 1950.
8. Sittler, R. W., "System Analysis of Discrete Markov Process," IRE, PGCT, Vol. CT-3, No. 4 (December 1956), pp. 257-266.
9. Howard, R. A., Dynamic Programming and Markov Processes, M. I. T. Press and John Wiley and Sons, 1960.
10. Gill, A., EE263 lectures, Spring 1961, at the University of California, Berkeley.
11. Kaneko, H., EE290E Term Paper, "Application of the z-Transform Theories for the Finite-State Markov Process," submitted to Prof. E. I. Jury, December 30, 1961.
12. Kaneko, H., EE290A Term Paper, "A Few Probabilistic Input-Output Relations of Deterministic Finite-State-Machine Elements," submitted to Prof. L. A. Zadeh, January 15, 1962.

## DISTRIBUTION LIST
## CONTRACT NO. AF 19(604)-5466

| ORGANIZATION | NO. COPIES |
|---|---|
| AFMTC (AFMTC Tech Library-MU-135)<br>Patrick AFB, Florida | 1 |
| AUL<br>Maxwell AFB, Alabama | 1 |
| OAR (RROS, Col. John R. Fowler)<br>Tempo D<br>4th and Independence Avenue<br>Washington 25, D. C. | 1 |
| AFOSR, OAR (SRYP)<br>Tempo D<br>4th and Independence Avenue<br>Washington 25, D. C. | 1 |
| ASD (ASAPRD - Dist)<br>Wright-Patterson AFB, Ohio | 1 |
| RADC (RAYLD)<br>Griffiss AFB, New York<br>ATTN: Documents Library | 1 |
| AF Missile Development Center (MDGRT)<br>Holloman AFB, New Mexico | 1 |
| Hq. OAR (RROSP, Maj. Richard W. Nelson)<br>Washington 25, D. C. | 1 |
| ARL (ARA-2)<br>Library AFL 2292<br>Building 450<br>Wright-Patterson AFB, Ohio | 1 |
| Commanding General<br>USASRDL<br>Ft. Monmouth, New Jersey<br>ATTN Tech Doc. Ctr.<br>SIGRA/SL-ADT | 1 |
| Department of the Army<br>Office of the Chief Signal Officer<br>Washington 25, D. C.<br>ATTN. SIGRD-4a-2 | 1 |
| Commanding Officer<br>Diamond Ordnance Fuze Laboratories<br>Washington 25, D. C.<br>ATTN: ORDTL-012 | 1 |
| Redstone Scientific Information Center<br>U. S. Army Missile Command<br>Redstone Arsenal, Alabama | 1 |
| Office of Scientific Intelligence<br>Central Intelligence Agency<br>2430 E Street, N. W.<br>Washington 25, D. C. | 1 |
| ASTIA (TIPAA)<br>Arlington Hall Station<br>Arlington 12 Virginia | 10 |
| Scientific and Technical Information Facility<br>P. O. Box 5700<br>Bethesda, Maryland<br>ATTN NASA Representative (S-AK/DL) | 1 |
| Director<br>Langley Research Center<br>National Aeronautics and Space Administration<br>Langley Field, Virginia | 1 |
| Chief, Bureau of Naval Weapons<br>Department of the Navy<br>Washington 25, D.C.<br>ATTN: DLI-31 | 2 |
| Director (Code 2027)<br>U. S. Naval Research Laboratory<br>Washington 25, D. C. | 2 |
| Director, USAF Project RAND<br>The Rand Corporation<br>1700 Main Street<br>Santa Monica, California<br>THRU: AF Liaison Office | 1 |
| AFCRL, OAR (CRXRA - Stop 39)<br>L. G. Hanscom Field<br>Bedford, Massachusetts | 10 |
| Technical Information Office<br>European Office, Aerospace Research<br>Shell Building<br>47 Cantersteen<br>Brussels, Belgium | 1 |
| U. S. Army Aviation Human Research Unit<br>U. S. Continental Army Command<br>P. O. Box 428,<br>Fort Rucker, Alabama<br>ATTN: Major Arne H. Eliasson | 1 |
| Technological University<br>Kanaalweg 2B<br>Delft, Netherlands<br>ATTN: Dr. Pieter Eykhoff<br>Department of Electrical Engineering | 1 |
| Library<br>Boulder Laboratories<br>National Bureau of Standards<br>Boulder, Colorado | 2 |
| Institute of the Aerospace Sciences, Inc.<br>2 East 64th Street<br>New York 21, New York<br>ATTN: Librarian | 1 |
| AFCRL, OAR (CRXR, J. R. Marple)<br>L. G. Hanscom Field<br>Bedford, Massachusetts | 1 |
| Office of Naval Research<br>Branch Office, London<br>Navy 100, Box 39<br>F. P. O., New York, New York | 1 |
| Massachusetts Institute of Technology<br>Research Laboratory<br>Building 26, Room 327<br>Cambridge 39, Massachusetts<br>ATTN: John H. Hewitt | 1 |
| Alderman Library<br>University of Virginia<br>Charlottesville, Virginia | 1 |
| Defence Research Member<br>Canadian Joint Staff<br>2450 Massachusetts Avenue, N. W.<br>Washington 8, D. C. | 1 |
| American Systems Incorporated<br>1625 East 126th Street<br>Hawthorne, California<br>ATTN: M. D. Adcock, Director<br>Electromagnetic Systems Division | 1 |
| Major General Casemiro Montenegro Filho, Director<br>Centro Tecnico da Aeronautica (CTA)<br>San Jose dos Campos<br>Sao Paulo, Brazil | 1 |
| The Ohio State University<br>Antenna Laboratory<br>2024 Neil Avenue<br>Columbus 10, Ohio<br>ATTN: Security Officer | 1 |
| Princeton University<br>School of Engineering<br>Princeton, New Jersey<br>ATTN: Miss Karen Takle, Librarian<br>The Engineering Library | 1 |
| AFOSR (Harold Wooster)<br>Director, Research Information Office<br>Washington 25, D. C. | 1 |
| WADD (WOLJR)<br>Wright-Patterson AFB, Ohio<br>ATTN: Mr. R. M. Lemmen | 1 |
| RADC (RCWID)<br>Griffiss AFB, New York<br>ATTN: Capt. D. J. Long | 1 |
| Atomic Energy Commission (John R. Pasta)<br>Division of Research<br>Washington 25, D. C. | 1 |
| 496L SPO (Space Track)<br>(ESSIS, Stop 2)<br>424 Trapelo Road<br>Waltham 54, Massachusetts | 1 |
| National Science Foundation<br>Engineering Sciences Program<br>1951 Constitution Avenue<br>Washington 25, D. C. | 1 |
| ESD (ESRDD, Major W. Harris)<br>L. G. Hanscom Field<br>Bedford, Massachusetts | 1 |
| Office of Naval Research<br>Information Systems Branch<br>Washington 25, D. C.<br>ATTN: Code 437, Marshall C. Yovits | 1 |
| AFCRL, OAR (CRRB, Dr. H. Zschirnt)<br>L. G. Hanscom Field<br>Bedford, Massachusetts | 7 |

Electronics Research Directorate, Air Force Cambridge Research Laboratories, Office of Aerospace Research, U.S. Air Force, Bedford, Mass.
Rpt. No. AFCRL-62-939, A FEW PROBABILISTIC PROPERTIES OF MODULAR CIRCUITS
Interim Report, April 62, 30 p., incl. illus., 12 refs.

Unclassified Report

Output probabilities of finite-state-machine elements are studied when the input of the machine elements is a random process. Delay element, modulo m adder and modulo m multiplier are considered as the machine elements. A new approach to the problem is made by defining the transformation matrices $\underset{\sim}{T}$ and $\underset{\sim}{U}$ for a modulo m adder and a modulo m multiplier respectively. By using these matrices, the output probabilities of the machine and the stochastic matrix of the output are given in explicit expressions, assuming that the input process is a finite-state, time-invariant Markov process. A few examples of the combinatorial circuit of these elements are also studied.

1. Digital Systems
2. Markov Chains
3. Statistical Analysis
I. AFCRL Project No. 5632
Task No. 56320
II. Contract AF 19(604)-5466
III. Univ. of California, Berkeley, Calif.
IV. Kaneko, H.
V. ERL Series No. 60, Issue No. 448
VI. Aval fr OTS: $1.25
VII. In ASTIA collection

Electronics Research Directorate, Air Force Cambridge Research Laboratories, Office of Aerospace Research, U.S. Air Force, Bedford, Mass.
Rpt. No. AFCRL-62-939, A FEW PROBABILISTIC PROPERTIES OF MODULAR CIRCUITS
Interim Report, April 62, 30 p., incl. illus., 12 refs.

Unclassified Report

Output probabilities of finite-state-machine elements are studied when the input of the machine elements is a random process. Delay element, modulo m adder and modulo m multiplier are considered as the machine elements. A new approach to the problem is made by defining the transformation matrices $\underset{\sim}{T}$ and $\underset{\sim}{U}$ for a modulo m adder and a modulo m multiplier respectively. By using these matrices, the output probabilities of the machine and the stochastic matrix of the output are given in explicit expressions, assuming that the input process is a finite-state, time-invariant Markov process. A few examples of the combinatorial circuit of these elements are also studied.

1. Digital Systems
2. Markov Chains
3. Statistical Analysis
I. AFCRL Project No. 5632
Task No. 56320
II. Contract AF 19(604)-5466
III. Univ. of California, Berkeley, Calif.
IV. Kaneko, H.
V. ERL Series No. 60, Issue No. 448
VI. Aval fr OTS: $1.25
VII. In ASTIA collection

Electronics Research Directorate, Air Force Cambridge Research Laboratories, Office of Aerospace Research, U.S. Air Force, Bedford, Mass.
Rpt. No. AFCRL-62-939, A FEW PROBABILISTIC PROPERTIES OF MODULAR CIRCUITS
Interim Report, April 62, 30 p., incl. illus., 12 refs.

Unclassified Report

Output probabilities of finite-state-machine elements are studied when the input of the machine elements is a random process. Delay element, modulo m adder and modulo m multiplier are considered as the machine elements. A new approach to the problem is made by defining the transformation matrices $\underset{\sim}{T}$ and $\underset{\sim}{U}$ for a modulo m adder and a modulo m multiplier respectively. By using these matrices, the output probabilities of the machine and the stochastic matrix of the output are given in explicit expressions, assuming that the input process is a finite-state, time-invariant Markov process. A few examples of the combinatorial circuit of these elements are also studied.

1. Digital Systems
2. Markov Chains
3. Statistical Analysis
I. AFCRL Project No. 5632
Task No. 56320
II. Contract AF 19(604)-5466
III. Univ. of California, Berkeley, Calif.
IV. Kaneko, H.
V. ERL Series No. 60, Issue No. 448
VI. Aval fr OTS: $1.25
VII. In ASTIA collection

Electronics Research Directorate, Air Force Cambridge Research Laboratories, Office of Aerospace Research, U.S. Air Force, Bedford, Mass.
Rpt. No. AFCRL-62-939, A FEW PROBABILISTIC PROPERTIES OF MODULAR CIRCUITS
Interim Report, April 62, 30 p., incl. illus., 12 refs.

Unclassified Report

Output probabilities of finite-state-machine elements are studied when the input of the machine elements is a random process. Delay element, modulo m adder and modulo m multiplier are considered as the machine elements. A new approach to the problem is made by defining the transformation matrices $\underset{\sim}{T}$ and $\underset{\sim}{U}$ for a modulo m adder and a modulo m multiplier respectively. By using these matrices, the output probabilities of the machine and the stochastic matrix of the output are given in explicit expressions, assuming that the input process is a finite-state, time-invariant Markov process. A few examples of the combinatorial circuit of these elements are also studied.

1. Digital Systems
2. Markov Chains
3. Statistical Analysis
I. AFCRL Project No. 5632
Task No. 56320
II. Contract AF 19(604)-5466
III. Univ. of California, Berkeley, Calif.
IV. Kaneko, H.
V. ERL Series No. 60, Issue No. 448
VI. Aval fr OTS: $1.25
VII. In ASTIA collection